



CHAPTER **3To**

Configuring Service Monitor

The following topics are included:

- [Configuring Trap Receivers, page 3-1](#)
- [Understanding and Setting Unified Communications Manager Credentials, page 3-2](#)
- [Selecting Sensors and Clusters to Monitor, page 3-11](#)
- [Configuring and Viewing Other Settings, page 3-15](#)



Note

For more information, see [Managing Sensors, page 4-1](#) and [Configuration Checklists and Tips, page A-1](#).

Configuring Trap Receivers

- Step 1** Select **Configuration > Trap Receivers**. The Trap Receiver Parameters page appears.
- Step 2** Enter the data described in the following table.

GUI Element	Description/Action
SNMP Community String	Enter the SNMP community string for each trap receiver.
Trap Receiver <i>n</i> and Port fields (where <i>n</i> is a number from 1 to 4)	<p>Enter up to 4 trap receivers:</p> <ul style="list-style-type: none"> • Trap Receiver <i>n</i>—Enter the IP address or DNS name of a server. To use Operations Manager to act on and display data from Service Monitor—for example to use the Service Quality Alerts dashboard—specify the IP address for the system with Operations Manager. • Port—Enter the port number on which the receiver listens for SNMP traps. The default is 162; however, a different port might be used for this purpose on this server. <p>When Service Monitor generates SNMP traps, it forwards them to these receivers.</p>

Step 3 Click **OK**.

Understanding and Setting Unified Communications Manager Credentials

For Service Monitor to obtain and analyze voice data from supported versions of Unified Communications Manager, you must provide credentials for the Unified Communications Manager publisher server. Any time that credentials on the Unified Communications Manager change, you must update the corresponding credentials in Service Monitor.

Step 1 Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page displays the information in the following table.

Columns or Buttons	Description/Action
Display Name	The user-specified name entered when credentials were added to Service Monitor.
IP Address	Cluster IP address.
Cluster	Version—Unified Communications Manager software version. ID—ID assigned to the cluster by Unified Communications Manager.
Last Contact Status	<p>One status is displayed for each credential that Service Monitor uses to contact the Unified Communications Manager cluster. Click any of the following statuses to open a dialog box with more information about the credential:</p> <ul style="list-style-type: none"> • Success • Verifying • Waiting for Data • Failure <p>If the status is blank, the credential is not required for Service Monitor to obtain information from this version of Unified Communications Manager. For more information, see Understanding Last Contact Status and When to Verify Credentials, page 3-4.</p> <p>The credentials are:</p> <ul style="list-style-type: none"> • HTTP/S—Indicates status of authentication to Unified Communications Manager Administration on the publisher server; applicable to Unified Communications Manager 4.x and later. • CDR/CDRM DB—Indicates status of authentication to one of these databases: <ul style="list-style-type: none"> – CDR—Applicable to Unified Communications Manager 4.x and earlier. – CDRM—Applicable to Unified Communications Manager 5.x and later. Service Monitor should gain access to the credentials for this database after providing the correct HTTP/S credentials. • Device DB—Applicable to Unified Communications Manager 3.3.x and earlier.
Buttons	<ul style="list-style-type: none"> • Add—Add credentials for a Unified Communications Manager cluster. See Adding Unified Communications Manager Credentials, page 3-5. • Edit—Edit credentials for a Unified Communications Manager cluster. See Editing Unified Communications Manager Credentials, page 3-9. • Delete—See Deleting Unified Communications Manager Credentials, page 3-10. • Verify—Verify credentials for a selected Unified Communications Manager cluster. See Understanding Last Contact Status and When to Verify Credentials, page 3-4. • Refresh—Refresh the page.

Understanding Last Contact Status and When to Verify Credentials

Service Monitor needs one or more credentials to obtain Unified Communications Manager data successfully. The Unified Communications Manager Credentials page displays the status of the last contact between Service Monitor and each Unified Communications Manager. If not blank, the status is a clickable link that opens a dialog box with more information that:

- Includes the last time Service Monitor tried to contact Unified Communications Manager and the last time Service Monitor was successful in making contact.
- Might indicate that Service Monitor is discarding data. Service Monitor discards data when receiving old data from Unified Communications 5.x and 6.x. This can happen after the connection between Service Monitor and Unified Communications Manager is reestablished after a break. Unified Communications Manager first sends older files to Service Monitor.

If the last contact status is not Success:

- The dialog box that is available from the clickable status might contain information that will help you to resolve the problem.
- Some potential issues to consider follow:
 - Service Monitor must be able to resolve the IP address for Unified Communications Manager to obtain the correct name. Verify that DNS parameters are specified correctly on the Service Monitor server and the Unified Communications Manager hostname has been added to DNS *or* supply the Unified Communications Manager hostname in the credentials. See [Supplying the Correct Hostname for Unified Communications Manager Credentials](#), page 3-8.
 - Known problems might exist that prevent successful data exchange between a cluster and Service Monitor. Check whether any have been identified in *Release Notes for Cisco Unified Service Monitor 2.1*.

In a few cases, you might need to correct credentials on Unified Communications Manager and then verify the credentials from Service Monitor:

- When the last contact status is Success, in some cases, Service Monitor might not be receiving data, but simply waiting to receive data. To see when the last successful contact occurred, click the status link. If the last contact was not recent, correct any problem with credentials on Unified Communications Manager and verify the credentials from Service Monitor.
- Credentials that Service Monitor relies upon might change on Unified Communications Manager platform. If this happens, check with your Unified Communications Manager administrator to obtain the correct credentials. If necessary, update the credentials in Service Monitor. Otherwise, verify the credentials.

Procedure

- Step 1** Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page appears.
 - Step 2** Select the Unified Communications Manager for which you want to verify credentials.
 - Step 3** Click **Verify**.
-

For more information, see the following topics:

- [Unified Communications Manager Configuration](#), page B-1
- [Understanding and Setting Unified Communications Manager Credentials](#), page 3-2

Supported Unified Communications Manager Versions

For the list of Unified Communications Manager versions that Service Monitor supports, see *Release Notes for Cisco Unified Service Monitor 2.1*.

Adding Unified Communications Manager Credentials

For Service Monitor to obtain and analyze voice data from supported versions of Unified Communications Manager, you must:

1. Perform configuration tasks either using Unified Communications Manager or logged in to the system where Unified Communications Manager is installed. See [Unified Communications Manager Configuration, page B-1](#).
2. Add Unified Communications Manager credentials to Service Monitor using the procedure for the appropriate version:
 - [Adding Credentials for Unified Communications Manager 3.3.x and 4.x, page 3-5](#)
 - [Adding Credentials for Unified Communications Manager 5.x and Later, page 3-7](#)



Note Each cluster that you add to Service Monitor must have a unique cluster ID. You can view the cluster IDs in Service Monitor on the Unified Communications Manager Credentials page. To view the cluster ID for a Unified Communications Manager that you plan to add, see [Setting Unified Communications Manager Enterprise Parameters, page B-3](#).

Adding Credentials for Unified Communications Manager 3.3.x and 4.x

Before you can add credentials to Service Monitor, you must configure them in Unified Communications Manager. See [Configuring Database Authentication on Unified Communications Manager 4.x and 3.3.x Systems, page B-6](#).



Note Every cluster that you add to Service Monitor must have a unique cluster ID. You can see the cluster IDs already in use on the Unified Communications Manager Credentials page. To view the cluster ID for the Unified Communications Manager that you plan to add, see [Setting Unified Communications Manager Enterprise Parameters, page B-3](#).

When you add credentials to Service Monitor, you must select the database authentication mode that corresponds to the one configured in Unified Communications Manager. See [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System, page B-6](#).

- Step 1** Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page appears.
- Step 2** Click **Add**. The Add Communications Manager dialog box appears.
- Step 3** Enter the data described in the following table.

Display Name	Enter a name—up to 20 characters—to describe the cluster.
Publisher Host Name	<p>(Optional) Enter the hostname for the publisher in the cluster.</p> <p>Note Service Monitor must be able to resolve the IP address for Unified Communications Manager to the correct name. If DNS parameters are specified correctly on the Service Monitor server and the Unified Communications Manager hostname has been updated in DNS, you do not need to enter the hostname here. To obtain the correct hostname to enter, see Supplying the Correct Hostname for Unified Communications Manager Credentials, page 3-8.</p>
Publisher IP Address	Enter the IP address for the publisher in the cluster.
Version	<p>Select the software version that runs on the cluster from these:</p> <ul style="list-style-type: none"> • CM 3.3.x • CM 4.x <p>Note For more information, see Supported Unified Communications Manager Versions, page 3-5.</p>
CDR Database (Displayed when you select version CM 4.x)	<p>Select the authentication mode that corresponds to the one used on Unified Communications Manager—see Determining Authentication Mode in Use on a Unified Communications Manager 4.x (or 3.3.x) System, page B-6—and enter any required data:</p> <ul style="list-style-type: none"> • Windows Authentication • SQL Authentication—When selected, you must also enter data in the SQL User Name and SQLPassword/Re-enter password fields. The usernames and passwords that you enter must match those entered for the Microsoft SQL Server account on the Unified Communications Manager publisher node; the account must have access to the CDR database.

HTTP/S User Name/Password/Re-enter password (Displayed when you select version CM 4.x)	Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server.
Database (Displayed when you select version CM 3.3.x)	Select the authentication mode that corresponds to the one used on the Unified Communications Manager system: <ul style="list-style-type: none"> • Windows Authentication—You do not need to enter any other information in Service Monitor. • SQL Authentication—If selected, the usernames and passwords that you enter must match those entered for Microsoft SQL Server accounts on the Unified Communications Manager publisher node: <ul style="list-style-type: none"> – SQL CDR-DB User Name and SQLCDR-DB Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account that has access to the CDR database. – SQL Device-DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account that has access to the device database. <p>Note The username and password for the CDR database and the device database will be the same if you have configured one Microsoft SQLServer account to access both databases.</p> <p>For more information, see Adding Microsoft SQLServer User Accounts for Unified Communications Manager 3.3.x and 4.x, page B-9</p>

Step 4 Click **OK**.



Note If Service Monitor fails to add the Unified Communications Manager credentials because a duplicate cluster ID exists, change the cluster ID as described in [Setting Unified Communications Manager Enterprise Parameters, page B-3](#) and add the Unified Communications Manager credential again. Every cluster added to Service Monitor must have a unique cluster ID.

Adding Credentials for Unified Communications Manager 5.x and Later



Caution

Before adding credentials for a Unified Communications Manager 5.x, 6.x, or 7.x software version cluster, confirm that the cluster ID does not include a space. For more information, see *Release Notes for Cisco Unified Service Monitor 2.1*.



Note For Unified Communications Manager 5.x and later, in addition to adding credentials using the following procedure, you must also provide an SFTP password. See [Configuring and Viewing Other Settings, page 3-15](#).

- Step 1** Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page appears.
- Step 2** Click **Add**. The Add Communications Manager dialog box appears.
- Step 3** Enter the data described in the following table.

Field	Description
Display Name	Enter a name—up to 20 characters—to describe the cluster.
Publisher Host Name	(Optional) Enter the hostname for the publisher in the cluster. Note Service Monitor must be able to resolve the IP address for Unified Communications Manager to the correct name. If DNS parameters are specified correctly on the Service Monitor server and the Unified Communications Manager hostname has been updated in DNS, you do not need to enter the hostname here. To obtain the correct hostname to enter, see Supplying the Correct Hostname for Unified Communications Manager Credentials, page 3-8 .
Publisher IP Address	Enter the IP address for the publisher in the cluster.
Version	Select this version: CM 5.x, 6.x, 7.x Note For more information, see Supported Unified Communications Manager Versions, page 3-5 .
HTTP/S User Name/Password/Re-enter Password	Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server. The user role must have Standard AXL API Access privilege.

- Step 4** Click **OK**.



Note If Service Monitor fails to add the Unified Communications Manager credentials because a duplicate cluster ID exists, change the cluster ID as described in [Setting Unified Communications Manager Enterprise Parameters, page B-3](#) and add the Unified Communications Manager credential again. Every cluster added to Service Monitor must have a unique cluster ID.

Supplying the Correct Hostname for Unified Communications Manager Credentials

To obtain the correct hostname to enter in Unified Communications Manager credentials, use the following procedure. If you do not have access to Unified Communications Manager Administration, contact a user who can do this and provide you with the correct name.

-
- Step 1** Log in to Unified Communications Manager Administration.
- Step 2** Select **System > Server** and find the page for the Unified Communications Manager. The name displayed on this page is the one you should enter in the Unified Communications Manager credentials in Service Monitor.
-

Editing Unified Communications Manager Credentials

- Step 1** Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page appears.
- Step 2** Select a cluster and click **Edit**. The Edit Unified Communications Manager dialog box appears.
- Step 3** Enter the data described in the following table.

Field	Description
Display Name	Enter a name—up to 20 characters—to describe the cluster.
Publisher Host Name	<p>Hostname for the server where Unified Communications Manager is installed.</p> <p>Note If Service Monitor successfully retrieves the hostname from Unified Communications Manager, it is displayed here, replacing any previously supplied hostname. If the hostname is not displayed here, you must enter it; see Supplying the Correct Hostname for Unified Communications Manager Credentials, page 3-8.</p>
Publisher IP Address	This field is grayed out because you cannot edit it.

Field	Description
Windows Authentication SQL Authentication (Displayed if version CM 3.3.x or CM 4.x was selected when adding credentials)	<p>Unified Communications Manager database authentication mode—Select either Windows Authentication or SQL Authentication.</p> <p>Note If you are considering changing the authentication mode, see Determining Authentication Mode in Use on a Unified Communications Manager 4.x (or 3.3.x) System, page B-6.</p> <p>If SQL authentication is selected, the usernames and passwords that you enter must match those entered for Microsoft SQL Server accounts on the Unified Communications Manager publisher node:</p> <ul style="list-style-type: none"> • SQL User Name and Password/Re-enter SQL Password—Enter the username and password for a Microsoft SQL Server account with access to the CDR database on the Unified Communications Manager version 4.x publisher node. • SQL CDR-DB User Name and SQLCDR-DB Password/Re-enter password—Enter the username and password for a Microsoft SQL Server account with access to the CDR database on the Unified Communications Manager version 3.3.x publisher node. • SQL Device-DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQL Server account with access to the device database on the Unified Communications Manager version 3.3.x publisher node. <p>Note The username and password for the CDR database and the device database will be the same if you have configured one Microsoft SQLServer account to access both databases.</p> <p>For more information, see Adding Microsoft SQLServer User Accounts for Unified Communications Manager 3.3.x and 4.x, page B-9.</p>
HTTP/S	<p>Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server.</p> <p>Note For Unified Communications Manager 5.x and later, the user role must have Standard AXL API Access privilege.</p>

Step 4 Click **OK**.

Deleting Unified Communications Manager Credentials

After you complete this procedure, Service Monitor can no longer obtain voice quality transmission data for the related cluster. Additionally, the cluster will no longer appears on the Monitored Phones page. Call data for the cluster remains in the database until it is purged. For more information, see [Maintaining the Service Monitor Database, page 6-1](#).

Before you complete this procedure, delete the cluster from any CVTQ threshold groups. See [Editing a CVTQ Threshold Group, page 5-6](#).

-
- Step 1** Select **Configuration > Unified Communications Manager Credentials**. The Unified Communications Manager Credentials page appears.
- Step 2** Select the check box by the cluster that you want to delete.
- Step 3** Click **Delete**. One of the following occurs:
- A confirmation dialog box appears.
 - An error message appears, displaying a list of CVTQ threshold groups to which the cluster belongs. You will need to remove the cluster from these CVTQ threshold groups and repeat this procedure.
- Step 4** Click **OK**.
-

Selecting Sensors and Clusters to Monitor

On the Monitored Phones page, you can view the total number of phones that Service Monitor is monitoring. You can also view the names of all sensors and Unified Communications Manager clusters known to Service Monitor, see whether each is monitored, and, if so, see the number of phones that Service Monitor manages in the cluster or for the sensor.

**Note**

Because it is possible for a Unified Communications Manager cluster and a sensor to report MOS for some of the same phones:

- The total known phone count displayed on the Monitored Phones page might be less than the sum of known phone counts for clusters/sensors.
 - To decrease the total known phone count, you might need to suspend more than one cluster or sensor.
-

- Step 1** Select **Configuration > Monitored Phones**. The Monitored Phones page appears, displaying the information in the following table.

GUI Element	Description
Total known phone count: (n)	Number of phones that Service Monitor is monitoring. If the number of phones equals the license size, the following message is displayed in red: Total known phone count (n) has reached or exceeded licensed limit! For more information, see Determining License Size Exceeded, page D-3 .
License limit: (n)	Number of phones allowed by license.
Cluster/Sensor List	
Cluster/Sensor ID column	One of the following: <ul style="list-style-type: none"> Cluster ID—The cluster ID is assigned by Unified Communications Manager. Sensor ID—Sensor MAC address.
Version column	Software version of Unified Communications Manager.
Type	One of the following: <ul style="list-style-type: none"> Cluster Sensor
State column	One of these: <ul style="list-style-type: none"> Monitored—Service Monitor is collecting and analyzing data from this cluster or sensor and sending traps when violations occur. Suspended—Service Monitor is not collecting and analyzing data from this cluster or sensor for one of these reasons: <ul style="list-style-type: none"> A user set the state of the cluster or sensor to Suspended. See Suspending and Resuming a Cluster or Sensor from Monitoring, page 3-12. Service Monitor could not monitor any more newly created clusters or phones when data was received because the phone license count was reached.

Suspending and Resuming a Cluster or Sensor from Monitoring

Provided that Unified Communications Manager is configured properly and Service Monitor license limits are not exceeded, Service Monitor starts to monitor a cluster when it learns of the cluster. Service Monitor learns of a cluster when you add Unified Communications Manager credentials to Service Monitor. (For more information, see [Adding Unified Communications Manager Credentials, page 3-5](#).)

Service Monitor learns of a sensor when the sensor registers.

If you want to suspend a cluster or a sensor from monitoring—for example, to enable you to monitor phones from a different cluster or sensor—you can do so.

Suspending a Cluster or Sensor

When you suspend a cluster or sensor, the following occurs:

- Data for the suspended cluster or sensor no longer appears in Service Monitor reports.
- The cluster or sensor appears on the Monitored Phones page as Suspended and the known phone count for that cluster or sensor drops to zero (0). If, as a result, the total known phone count also decreases, you are free to monitor additional phones in other clusters or from other sensors (up to your license limit).

-
- Step 1** Select **Configuration > Monitored Phones**.
- Step 2** Select the check box for the cluster or sensor that you want to suspend.
- Step 3** Click **Suspend**. A confirmation dialog box appears.
- Step 4** Click **OK**.
-

Resuming a Cluster or Sensor

-
- Step 1** Select **Configuration > Monitored Phones**.
- Step 2** Select the check box for a suspended cluster or sensor that you want to monitor.
- Step 3** Click **Resume**. A confirmation dialog box appears.
- Step 4** Click **OK**.
-

Updating the Total Known Phone Count for a Cluster

Service Monitor monitors the first n phones that it finds in the data that it receives or obtains from the clusters. If a phone in a cluster fails and is replaced, Service Monitor is not notified and continues to include the failed phone in the total known phone count. To refresh the total known phone count for a cluster, suspend the cluster and resume it.

**Note**

Suspending a cluster resets the phone count to zero for that cluster. The phone count then increases as and when calls come from a phone.

Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports

Use this procedure to configure:


- The number of endpoints to be included in CVTQ and sensor most-impacted endpoint reports no matter when they run—daily, weekly, or on demand.

- The most-impacted endpoints reports to export—CVTQ or sensor or both. Most-impacted endpoint reports can run daily and weekly, exporting the results to a comma-separated values file (CSV) or a portable document format (PDF) file. You can save the reports on the server and, optionally, automatically send them through e-mail.

**Note**

The maximum number of records that can be exported to a PDF file is 2,000. The maximum number of records that you can export to CSV is configurable; the default is 30,000 with an upper limit of 64,000 records. For more information, see [Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-17](#).

- Step 1** Select **Configuration > Export Settings**. The Export Settings (for Most Impacted Endpoint) page appears, displaying the information described in the following table.

GUI Element	Description/Action
Number of Endpoints field	Enter the number of endpoints that you want to see on all—exported or directly launched—most-impacted endpoints reports.
Daily at 1:00 AM check boxes	To generate the report every day, select at least one of the following: <ul style="list-style-type: none"> • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format. If neither is selected, Service Monitor does not generate the reports.
Weekly at 1:00 AM Monday check boxes	To generate the report every week, select at least one of the following: <ul style="list-style-type: none"> • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format. If neither is selected, Service Monitor does not generate the reports.
Report Type	Select at least one of the following: <ul style="list-style-type: none"> • Sensor • CVTQ <p>Note Separate reports are generated for sensor and CVTQ data. For report filenames, see Table 3-1.</p>
Save at	Enter a location for storing the reports on the server where Service Monitor is installed; a default location is displayed. <div style="text-align: center;">  </div> <p>Caution If you configure export settings to save files outside of <i>NMSROOT</i>, be sure to also log into the Service Monitor server, create the folder that you entered on the Export Settings page, and provide write permission to the folder for the user <i>casuser</i>. If you do not, Service Monitor cannot create the export files. (NMSROOT is the location where Service Monitor is installed. If you used the default location, it is C:\Program Files\CSCOpX.)</p>
E-mail to	(Optional) Enter one or more complete e-mail addresses separated by commas.
SMTP Server	(Optional) Enter an SMTP server.

Step 2 Click **Apply**.

Depending on the reports and formats that you have selected, the following reports will be generated.

Table 3-1 *Most-Impacted Endpoints Exported Reports*

Report Type	When Generated	Report Filenames
CVTQ	Daily	CVTQ_Daily_ddmmyyyy.csv
		CVTQ_Daily_ddmmyyyy.pdf
	Weekly Note Generated on Monday.	CVTQ_Weekly_ddmmyyyy.csv
		CVTQ_Weekly_ddmmyyyy.pdf
Sensors	Daily	Sensor_Daily_ddmmyyyy.csv
		Sensor_Daily_ddmmyyyy.pdf
	Weekly Note Generated on Monday.	Sensor_Weekly_ddmmyyyy.csv
		Sensor_Weekly_ddmmyyyy.pdf

Configuring and Viewing Other Settings

Use this procedure to:


- View some settings that are configured outside of the user interface. (See [Configuring Diagnostic Report Search and CSV Export Limit Settings](#), page 3-17 and [Configuring Low-Volume Schedule and Database Purging](#), page 6-1.)
- Configure SFTP settings if you are monitoring calls from Unified Communications Manager version 5.x or later.
- Enable the launch of Operations Manager from Service Monitor reports.

Step 1 Select **Configuration > Other Settings**. The Other Settings page appears.

Step 2 View settings and update SFTP settings as described in the following table:

Fields	Description/Action
Low-Volume Schedule Hours	
<day> <timerange>; <timerange> For example: Mon 0-6; 22-24	For each day of the week, timerange indicates the hours during which Service Monitor processes fewer records, handling a number that is roughly 20% of records processed during a peak period. During the low-volume schedule, Service Monitor performs database maintenance. Note A windows user with access to the Service Monitor server can configure this schedule. See Configuring Low-Volume Schedule and Database Purging , page 6-1.

Fields	Description/Action
Miscellaneous	
Wait for Diagnostic Report (min)	Number of minutes that Service Monitor continues to search—when there is a large volume of data—before displaying the matching records found so far for a diagnostic report (a Cisco 1040 Sensor report or a CVTQ report). To configure this setting, see Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-17 .
Report Data Retention Period (days)	<p>Number of days that data is retained in the Service Monitor database before being purged. The default value depends on the configuration:</p> <ul style="list-style-type: none"> • Service Monitor alone on a server—7 days. • Service Monitor and Operations Manager on a server—3 days. <p>On the Service Monitor server, a user can change the value of the data-retention-days property in the <code>NMSROOT\qovr\qovrconfig.properties</code> file. (NMSROOT is the location where Service Monitor is installed. If you used the default location, it is <code>C:\Program Files\CSCOpX</code>.) To put changes into effect after you edit <code>qovrconfig.properties</code>, you must stop and start the QOVR process. While logged in to the server where Service Monitor is installed, from the command line, enter these commands:</p> <pre>pdterm QOVR pdexec QOVR</pre>
Operations Manager Server	<p>Enter the IP address for the Operations Manager server that Service Monitor is registered to.</p> <p>Note Even when Operations Manager and Service Monitor run on the same system, you must replace the default value, <code>localhost</code>, with the correct IP address.</p> <p>Entering the IP address enables users to launch the Detailed Device View page or the Phone Detail window in Operations Manager from Service Monitor reports. (See Understanding Sensor Reports, page 2-6 and Understanding CVTQ Reports, page 2-10.)</p> <p>Note To enable users to view Operations Manager windows without first logging in to Operations Manager, you can configure single sign-on. For more information, see Enabling Single Sign-On in <i>User Guide for CiscoWorks Common Services 3.0.5</i>.</p>
SFTP	
Username	<p>You cannot change the username from <code>smuser</code>.</p> <p>This same username, <code>smuser</code>, must be configured in Unified Communications Manager. See Adding Service Monitor to Unified Communications Manager 5.x (or 6.x or 7.x) as a Billing Server, page B-4.</p>

Fields	Description/Action
Change password check box	Select to change password. <div style="text-align: center;">  Caution </div> <p>The default password is smuser. If you change the password here, you must also change the password for smuser in Unified Communications Manager. See Adding Service Monitor to Unified Communications Manager 5.x (or 6.x or 7.x) as a Billing Server, page B-4.</p>
Password	Enter password.
Re-enter password	Re-enter password.

Step 3 Click **Apply**.

Configuring Diagnostic Report Search and CSV Export Limit Settings

Table 3-2 lists properties that affect diagnostic reports. A windows user with access to the Service Monitor server can change the values of these properties in the `NMSROOT\qovr\qovrconfig.properties` file.

Table 3-2 Diagnostic Report and Export Settings

Property	Description and Limit
WaitForDiagReport	Number of minutes that Service Monitor continues to search—when there is a large volume of data—before displaying the matching records found so far for a diagnostic report (a Cisco 1040 Sensor report or a CVTQ report). Default: 2. Maximum: 4. Note Service Monitor reports can display up to 2,000 records. To see additional records, you can export a diagnostic report to a CSV file.
ExportCSVLimit	Number of records that Service Monitor exports to a CSV file. Default: 30000. Maximum: 64000—This is approximately the maximum number of records that can be included in a CSV file that Excel can open.

After you edit `qovrconfig.properties`, to put changes into effect, you must stop and start the QOVR process. While logged in to the server where Service Monitor is installed, from the command line, enter these commands:

```
pdterm QOVR
pdexec QOVR
```

